Commonwealth Office of Technology

Security Awareness Newsletter

Published by the COT Division of Security Services

July 2004 Volume 11, Issue 3

Inside this issue:

July's Security Tip

Identity Theft Prevention

—Don't give out personal information to telephone or email solicitors.
—Make sure your PC has the latest security patches and virus definition files installed, as well as a personal firewall software.
—When using PCs at libraries, cyber cafés, etc., make sure you fully log off of a secure Web site. Simply closing down the browser may not be enough to prevent the next user from accessing the Web pages.
—When disposing of documents, always shred or burn pre-approved credit card offers, bank statements, receipts containing credit card info, etc.

For more info, visit the Identify Theft Resource Center

Managing Content and Combating Spam on the Commonwealth's Networks

The growth of the Internet and email has had a tremendous impact on how the Commonwealth conducts business today. While the benefits of these technologies are obvious to us all, there are increasing issues with inappropriate and/or offensive content that pose serious problems for Kentucky State Government.

Unsolicited messages (Spam), sexually or racially offensive email, non-business related and pornographic Web site access are all examples of activities that can negatively impact the Commonwealth by degrading network performance; burdening the email system; exposing the network to viruses, worms, and Trojans; and reducing employee productivity. There are also possible legal ramifications for the state if its employees view or distribute objectionable materials.

But help is on the way! In April 2004, the Commonwealth entered into a strategic partnership with Network Appliance, Inc. (NetApp) to provide a Content Security Management (CSM) solution that provides a means for the Commonwealth to manage its Internet and email content and better secure the network infrastructure.

COT plans to make CSM available to all state agencies by September 30, 2004.

The NetApp solution is comprised of its network caching appliances and the Webwasher CSM Suite that function in unison to provide:

—URL blocking to help reduce inappropriate Internet access.
—Email content filtering to reduce/eliminate Spam and other undesirable content on the Commonwealth's networks.
—Malicious code protection to ensure that Web and email content is virus free, providing an additional layer of virus protection to the network.
—Pop-up message and peer-to-peer application blocking.

In May 2004, the Commonwealth Office of Technology (COT) began a pilot implementation of the CSM solution in the Finance Cabinet, blocking access to inappropriate Internet sites. COT plans to make CSM available to all state government agencies by September 30, 2004.

For more information on the acceptable use of the State's Internet and email resources, refer to the Commonwealth's Enterprise Internet and Electronic Mail Acceptable Use Policy (CIO-060).

Contributor—Chris Johnson, COT LAN Team Manager

Did You Know . . .
According to ClickZ Stats, 80 percent of spam is likely generated from zombie PCs that are controlled by spam Trojan horses. These destructive programs are usually installed by worms or spyware without the user's knowledge.

Portable Device Security

The use of portable computing devices (laptops, PDAs, Blackberry devices, smart phones, etc.) is on the rise. Their convenience and functionality has made them very popular, particularly with mobile workers; however, there are security issues that should be addressed to avoid a possible security breach or compromise.

One issue of concern is the growing use of wireless technologies in these devices that extend the boundaries of the traditional network. Unless encryption is used, malicious hackers or eavesdroppers could 'sniff' wireless transmissions and harvest sensitive information.

Another security issue is the increased risk of theft. These devices are often expensive and small in size, making them an attractive target for thieves. The theft of a device can pose serious consequences, particularly if the device contains sensitive or confidential information. Although the Commonwealth does not currently have an enterprise policy on securing portable devices, agencies may want to enact internal policy that outlines ways to properly protect these devices. Some recommended security procedures include:

—Only devices owned by the Commonwealth should be connected to the Commonwealth's networks, computers, etc.

—Devices that are lost or stolen should be reported immediately to the appropriate agency staff in order for services to be deactivated and prevent possible security breach or compromise.

—Devices containing sensitive information should employ both hard disk encryption for all files, as well as boot protection via a password, where possible. *(Note: Highly sensitive/confidential information should not be stored on portable computing devices due to the increased risk of theft and wireless security issues.)*

—Sensitive information should not be transmitted to or from devices unless approved transmission protocols and security technologies are utilized, i.e., encryption, VPN, etc.

—Devices should be password protected. Boot and logon passwords should be employed where feasible. Password usage and composition rules should adhere to the Enterprise UserID and Password Policy (CIO-072).

—Inactivity/timeout settings that automatically lock the device should be enabled where possible. It is recommended that the setting should be configured to be invoked after 10 minutes of inactivity. Note: Exceptions to this requirement for Personal Digital Assistants (PDAs) may be considered where business requires a longer period of inactivity.

—Portable computing devices should be prohibited from use by anyone other than the Commonwealth employee to whom the device was assigned.

—Logging utilities, where possible, should be enabled when the devices are attached to or removed from Commonwealth assets. Logs detailing the data transferred to or copied from these devices should be maintained and reviewed periodically.

—Devices should employ current virus protection software and virus definition files, where feasible, and adhere to the Enterprise Anti-Virus Policy (CIO-073).

—Devices should be physically secured when not in use by locking them in desk drawers or other secure areas.

—Devices that use wireless technologies such as Bluetooth and 802.x should not broadcast their presence. In addition, the device's wireless network card should be disabled when not in use.

Did You Know . . .

According to the 2004 PDA Usage Survey conducted by Pepperdine University, 24 percent of respondents experienced a loss or theft of a PDA and 81 percent said they carry 'somewhat valuable' or 'extremely valuable' information on their handheld device.

Internet Phishing: How to Avoid Becoming the Catch of the Day

Phishing is a term used to describe the latest high-tech scam hitting the Internet these days. While Phishing has been around for a while, according to the research firm, Gartner Inc., 'phishing scams have exploded this year' with 76 percent of known or suspected attacks occurring within the past six months.

Unscrupulous individuals are using spam to trick email recipients into revealing sensitive information such as social security numbers, bank account information, credit card numbers, passwords and other confidential information. The emails are disguised as legitimate correspondence from businesses that ask potential victims to update their billing information to keep their accounts active. Scammers use this information to order items and obtain credit using the victim's financial identity.

. . . 'phishing scams have exploded this year' with 76 percent of known or suspected attacks occurring within the past six months.

The Federal Trade Commission offers the following tips to avoid Phishing scams:

—If you receive an email or popup message asking for personal or financial information, do not reply or click on the link in the message. Legitimate businesses usually do not ask for sensitive information via email. If you are concerned about your account, contact the business by telephone using a number you know to be genuine.

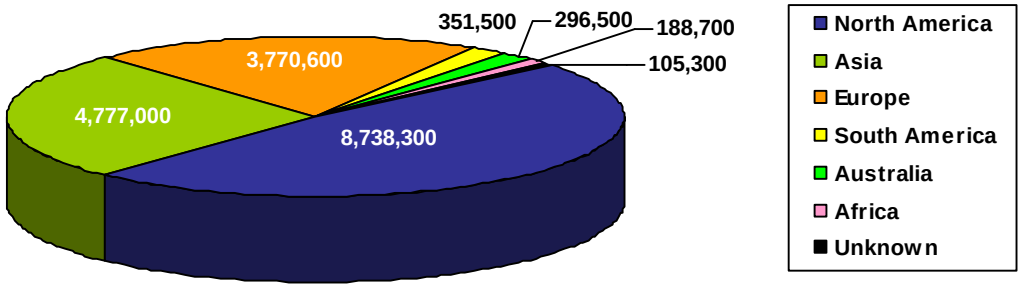
—Never email personal or financial information unless encryption is used. If you initiate a transaction and want to provide your personal or financial information through a business' Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a Web site that begins with 'https:'. Unfortunately, no indicator is foolproof—some phishers have forged security icons.

—Review credit card and bank statements as soon as you receive them to determine if there are any unauthorized charges. Use anti-virus software and keep it current. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a personal firewall can protect you from inadvertently accepting such unwanted files.

—Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them to you.

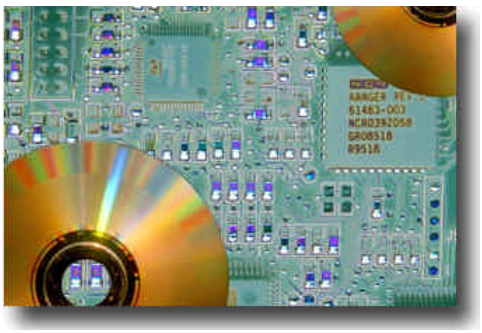
—COT recommends that any suspected phishing scam be reported to COT via a Security Incident Reporting Form. Suspicious activity can also be reported to the Federal Trade Commission. If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

Malicious Code Infections During the Past 30 Days By Region



Source: Trend Micro

Secure Configuration of Servers and Workstations



As new workstations and servers are configured, these devices are often connected to the Internet in order to access installation files on a network server and to download crucial security updates. Frequently, these unprotected devices are instantly infected with malicious code, especially by viruses and worms that exploit Microsoft vulnerabilities such as the Sasser and Nachi worms. Below are steps to securely configure unprotected devices prior to their introduction to the network:

1. Create installation CDs so the device can be configured before connecting to the network.
2. Install the operating system from CD.
3. Install the latest version of the anti-virus software from CD. That includes the most current engine and virus definition files (aka DATs).
4. Properly configure the anti-virus software to scan all files. (*Refer to the Commonwealth's Enterprise Anti-Virus Policy for complete configuration instructions.*)
5. Now the device can be connected to the network.
6. Install a host-based firewall (personal firewall) such as BlackIce.
7. Install the Microsoft operating system patches next.
8. At this point the system is reasonably well protected and normal configuration can resume.

If you would like more information on the secure installation of workstations and servers, refer to the CERT Coordination Center's tech tip article, 'Before You Connect a New Computer to the Internet.'

Contributors—Richard Grant and Joseph Rach, COT Security Engineers

---

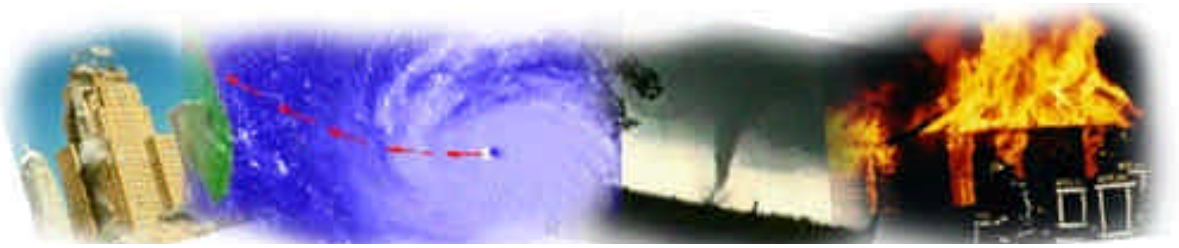
The Word on Trojans

According to TechWeb's TechEncylopedia, "A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer." Trojans are somewhat more dangerous than viruses and worms in that you may not realize they are on your computer. Trojans provide a back door to your PC that allows hackers to collect passwords, record keystrokes, view your screen, read and modify documents and even publish your hard drive on the Internet to share with others.

Trojans come disguised as pictures, games, screensavers and other executable files. Some well known Trojans are Back Orifice, NetBus and SubSeven. Infection vectors include email attachments and instant messaging programs such as ICQ. A recent Trojan attack affected a small number of Commonwealth workstations running IIS (Microsoft Internet Information Services) in late June 2004. This threat was part of a widespread attack involving many IIS servers across the Internet. The attack is believed to have originated from a for-profit Russian hacker organization and targeted IIS web servers, distributing a downloader program to Web site visitors' Microsoft Internet Explorer software. Keystroke loggers and other malicious programs were then installed on compromised systems.

While the majority of Trojan threats can be avoided by simply keeping your anti-virus software updated and systems appropriately patched, additional detection tools may be required to detect and remove newer Trojans. Be aware that Trojans are known to make registry or startup file changes in order that certain malicious files are executed on boot-up. Thoroughly research the Trojan to remove the tracks that it leaves behind. In addition to anti-virus software, a personal firewall such as Internet Security System's BlackICE can be used to stop Trojans before they compromise your computer.

For more information on Trojans, check out this Windows Security article.



Disaster Recovery—Defining the Threats

When you think of disaster recovery you may visualize terrorism as being the main reason behind a disaster recovery plan (DRP), especially after the September 11 attacks on the World Trade Center and the Pentagon. Terrorism is definitely a major concern during these times; however, power failures and storms actually account for over 50 percent of all declared disasters and are much more likely to occur. All of these threats, along with terrorism, are crucial reasons why a disaster recovery plan is necessary. You never know when one of these threats may become a reality and having an up-to-date plan that has been thoroughly tested and rehearsed can mean the difference between an organization's demise or survival after a catastrophic event.

The following is a list that outlines some types of potential threats:

Environmental Disasters	Deliberate/Security Incidents	Loss of Utilities and/or Services	Equipment or System Failure
Tornado	Act of Terrorism	Electrical Power Failure	Internal Power Failure
Hurricane	Workplace Violence	Communications Services	Air Conditioning Failure
Flood	Cyber Crime	Breakdown	Equipment Failure
Snowstorm	Loss of Records or Data	Supplier Failure	(excluding IT hardware)
Earthquake	Disclosure of Sensitive Info		
Electrical Storms			
Fire			
Freezing Conditions			

You may think that the threats mentioned above only happen at other companies, but COT has received seven reports of physical incidents occurring within the past year that involved unauthorized building access, fire and bomb threats. Thankfully, none of these incidents significantly impacted the Commonwealth's ability to deliver services, but if it had, COT would have had its DRP to provide staff with the guidance necessary to restore services in a timely manner.

Update—Hot/Cold Site Contract Awarded

On July 1, 2004, a new hot/cold site contract was awarded to IBM Recovery Services. This contract substantially moves the Commonwealth forward in its ability to recover from disaster situations and allows for coverage of all critical components. The principal benefits this contract brings to the Commonwealth are:

—96 hours of annual test time – a significant increase from the previous contract's 48 hours of test time.
—All critical hardware is covered except for network devices.
—All operating systems will be preloaded, potentially saving hours of time during recovery.
—New contract is considerably less expensive than equivalent current contract pricing.
—Includes a vendor managed DS1 and dial-up circuits for testing requirements. (DS1 is a classification of digital circuits comprised of 24 individual voice channels with a speed of 1.544 Mbps.)
—Offers an available remote test center.
—Offers 1,000 square feet of cold site space for distributed system build out if needed.
—Allows for the first ever integrated mainframe/distributed testing to be accomplished.

Contributors—Kristy Holliday and Tom Van Horn, COT Disaster Recovery Team

CYBER BYTES

Current Security News & Information

Phishing Attacks Becoming More Sophisticated

The latest phishing attacks are using legitimate Web sites to lure unsuspecting victims to divulge sensitive financial information. Citibank has earned the title of being the number one target for these fraudulent ploys. To learn more, read this article.

New Lovgate Variant Causes Havoc for Windows Applications

The latest Lovgate variants, Lovgate.AE and Lovgate.AH, rename executable files associated with various Windows applications, disabling compromised systems. For more information, check out the ZDNet article.

Note: McAfee provides protection for the various Lovgate versions in their latest virus definition file (DAT).

iPods Deemed a Security Risk for Business Use

The research firm, Gartner Inc., recommends that business organizations ban the use of iPods, Apple's digital music player. The device's use of USB or FireWire ports is behind Gartner's announcement. FireWire is a peripheral standard that can move large amounts of data between a computer and portable computing devices. Read the Network World Fusion article for more info.

Federal Ruling Shoots Down Email Privacy

A recent federal appeals court ruling states that copying email messages in transit is not a crime under the federal Wiretap Act. Read more.

2004 E-Crime Watch Survey Results

E-Crimes are up with organizations reporting $666 million in loses for 2003. Read more about the survey results at the CERT Web site.

NIST Releases Draft Guide for Securing Windows XP

NIST Special Publication 800-68 has been created to assist IT professionals in effectively securing XP systems. The guide provides insight into the threats and security controls that are relevant for various operational environments. To find out more about this publication, visit the NIST Web site.

Microsoft Updates

Microsoft has released the following security updates for its operating systems and other software products. COT recommends that agencies devise procedures to ensure the timely installation of hardware and software patches/updates, as well as the update of virus definition files (aka DATs). A comprehensive list of hardware and software security vulnerabilities affecting multiple platforms can be found on the COT Security Alerts Web page.

Microsoft Security Bulletin MS04-018

Cumulative Security Update for Outlook Express (823353)
Moderate—This update replaces MS04-013: Cumulative Update for Outlook Express and any prior cumulative security updates for Outlook Express.

Microsoft Security Bulletin MS04-019

Vulnerability in Utility Manager Could Allow Code Execution (842526)
Important—Affects Microsoft Windows 2000.

Microsoft Security Bulletin MS04-020

Vulnerability in POSIX Could Allow Code Execution (841872)
Important—Affects Microsoft Windows 2000 & Windows NT.

Microsoft Security Bulletin MS04-021

Security Update for IIS 4.0 (841373)
Important—Affects Windows NT 4.0.

Microsoft Security Bulletin MS04-022

Vulnerability in Task Scheduler Could Allow Code Execution (841873)
Critical—Affects Windows 2000 & XP.

Microsoft Security Bulletin MS04-023

Vulnerability in HTML Help Could Allow Code Execution (840315)
Critical—Affects Windows 2000, XP, 98, ME & Windows Server 2000.

Microsoft Security Bulletin MS04-024

Vulnerability in Windows Shell Could Allow Code Execution (839645)
Important—Affects Windows 2000, XP, NT, 98, ME & Windows Server 2000.

Upcoming Microsoft Webcast Offerings

Microsoft offers numerous free Webcasts on security-related topics. To learn more about upcoming live Webcasts, check out Microsoft's Web page. Please note that in order to view the Webcasts, you must first install Microsoft's Live Meeting software. Check out this Microsoft FAQ for more information on installing Live Meeting.

Automatically Update Your Computer

Windows Update allows you to automatically update your computer's operating system, software, and hardware with the latest security patches. To learn more, visit the Windows Update Site and follow the prompts.

COMMONWEALTH OFFICE OF TECHNOLOGY

Division of Security Services

101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502.564.7680

Email:
GOTSecurityServices @ky.gov

We're on the Web!
ky.gov/got/security/

The information contained in this newsletter is intended for internal use only.

The Commonwealth Office of Technology's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security & IT professionals with timely information on cyber vulnerabilities, information security trends, malicious code info, and security policies & best practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity, and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC), and other key state computing facilities.

Security Services is also responsible for the development and maintenance of COT's Security Policies and Procedures Manual (SPPM), disaster recovery/business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, 2003, and Unix Solaris & AIX systems. DSS also provides mainframe RACF support, incident management, disaster recovery administration, and a number of security awareness activities. If you would like to learn more about the services provided by DSS, visit our Web page at ky.gov/got/security.

For more information on IT Security, check out the following Web sites!

Fight Spam on the Internet—Site that has the latest anti-spam laws, information, and links to other resources.

HideAway.Net—Contains daily updates on the latest alerts, news and information in the world of Internet security, privacy online, and viruses.

SC Magazine Online—Online resource for IT security professionals.

SecuriTeam—Central security Web site containing all the newest security information from various mailing lists, hacker channels and their own tools and knowledge.

TechNewsWorld—Rated by Forbes Magazine as one of the top 10 technology news sites.

Virus Bulletin—Features independent anti-virus advice.

Webopedia—Online encyclopedia dedicated to computer technology.

Windows Security—Contains the lasts security articles on Microsoft Windows.